



DATA BREACH POLICY

Published:

DECEMBER 2025

ACKNOWLEDGEMENT OF COUNTRY

Hunter Water acknowledges the Traditional Countries of the Awabakal, Darkinjung, Geawegal, Wonnarua and Worimi peoples and the Countries on which we operate and beyond where our water flows.

We recognise and respect the cultural heritage, beliefs and continuing connection to the lands and waters of our Traditional Custodians and pay respect to their Elders past, present and emerging.



1 Introduction

Hunter Water Corporation (Hunter Water) has prepared and published this Data Breach Policy (DBP) in accordance with the requirements of the Mandatory Notification Data Breach (MNDB) Scheme detailed in Part 6A of the *Privacy and Personal Information Protection Act 1998* NSW (PIIP Act).

Hunter Water is committed to preventing and responding to data breaches in accordance with the requirements of the PIIP Act. Hunter Water acknowledges the value of personal information and its responsibility to ensure it is safeguarded and managed appropriately. The Hunter Water Privacy Framework has been developed to support all of Hunter Water's people to contribute to a privacy positive culture.

The Privacy Framework consists of the following Hunter Water documents:

- the Privacy Policy;
- the Privacy Management Plan;
- this DBP.

This DBP also forms part of the overarching Hunter Water Corporate Emergency Response Plan (CERP). The CERP details the organisation and management of resources for dealing with all aspects of emergency management. Specifically, the DBP details how Hunter Water will manage and respond to suspected or actual eligible data breaches (EDB) to ensure effective management of personal information and to fulfil legislative requirements.

This DBP aligns with Hunter Water's value of trust. Hunter Water recognises that our people, customers, stakeholders and community trust us to keep their personal information safe and secure. We respect this trust and work together to continually improve the way that we respond to privacy and security threats

2 Scope

This DBP sets out Hunter Water's approach to complying with the MNDB Scheme, roles and responsibilities for reporting data breaches, and strategies for containing, assessing and managing EDBs.

This DBP applies to all of Hunter Water's people (as defined in section 5) and to all third-party providers or contractors who hold personal information or health information on behalf of Hunter Water.

This DBP only applies to data breaches involving personal information or health information

3 Purpose

The purpose of this DBP is to provide guidance to Hunter Water's people on identifying, preventing and responding to data breaches of Hunter Water held data in accordance with the PIIP Act.

In particular, this DBP sets out the key actions and responsibilities for notifying, containing and managing an EDB pursuant to the MNDB Scheme.

This DBP details (among other matters):

- what constitutes a data breach, including an EDB under the PIIP Act;
- roles and responsibilities of Hunter Water's people (including for reporting, reviewing and managing data breaches);
- how Hunter Water has prepared for a data breach;
- the steps involved in reporting and responding to a data breach;
- Hunter Water's record keeping requirements;
- data post-breach review and evaluation activities, including reviewing systems, policies and procedures to prevent further data breaches.

This document does not substitute Hunter Water’s obligations under relevant laws, including the PPIP Act. The response to data breaches will be context specific and accordingly no template response can be applied in all cases.

4 Delegation

Under section 59ZJ of the PPIP Act, the ‘head of a public sector agency’ (that is, Hunter Water’s Managing Director) may delegate the exercise of a function of the head of the agency to a person employed in or by Hunter Water.

The Managing Director has delegated the Managing Director’s role in relation to the MNDB Scheme to the employee occupying the role of Legal Counsel and Privacy Officer.

The Managing Director and its delegate will be supported by Hunter Water’s Data Breach Response Team (DBRT). The DBRT will be comprised of the following roles (or such other roles as determined by the Managing Director):

- The General Counsel or Group Manager Legal
- Legal Counsel and Privacy Officer
- Group Manager Digital Services and Tech or Team Leader Information Security
- Group Manager Communications and Engagement
- Business Continuity Manager

5 Definitions, Acronyms and Abbreviations

For the purposes of this DBP, terms and phrases used in this document have the meaning set out below or as otherwise defined internally within this document:

Term or Phrase	Definition
Eligible Data Breach or EDB	Defined in section 59D of the PPIP Act. Refer also to section 8 of this DBP.
Health Information	As defined in section 6 of the <i>Health Records and Information Privacy Act 2002</i> (NSW).
Held	Personal information is in the possession or control of Hunter Water or the information is contained in a state record in respect of which Hunter Water is responsible under the <i>State Records Act 1998</i> (NSW).
Hunter Water’s people	Hunter Water’s officers, employees (including any individual employed by Hunter Water on a permanent, temporary or casual basis) and all individuals performing work in any capacity for Hunter Water, such as contractors, subcontractors, agents, consultants, and those undertaking work experience, secondments and volunteer work.
Personal Information	As defined in section 4 of the PPIP Act. In this document, ‘personal information’ includes health information.
Public sector agency	As defined in section 3 of the PPIP Act. For the purposes of the PPIP Act and the MNDB Scheme, Hunter Water is a public sector agency.
PPIP Act	<i>Privacy and Personal Information Protection Act 1998</i> NSW (PPIP Act)

6 Roles and Responsibilities

All of Hunter Water's people have a role to play in the prevention and management of data breaches. The following Hunter Water people have identified roles under the DBP:

Role(s)	Responsibilities
Managing Director or its delegate	Hunter Water's Managing Director or the Managing Director's delegate will carry out all responsibilities necessary to meet the obligations imposed on the head of a public sector agency under Part 6A of the PPIP Act.
Data Breach Response Team or DBRT	Hunter Water's DBRT will support the Managing Director or delegate in responding to, assessing and containing data breaches, including suspected EDBs. The DBRT will also assist Hunter Water to conduct post-breach reviews and evaluations and to test the effectiveness of this DBP.
Executive Manager People and Culture and Managing Learning and Capability	The Hunter Water Learning and Development Team in collaboration with the Legal and Privacy Team is responsible for ensuring all of Hunter Water's people are made aware of, and provided adequate training in, privacy-related matters, including their obligations under the MNDB Scheme and this DBP.
Legal and Privacy Team	The Hunter Water Legal and Privacy Team is responsible for implementing this DBP and ensuring that it is reviewed, tested and updated in accordance with the requirements of this DBP.
All Hunter Water's people (as defined)	All of Hunter Water's people are responsible for preventing data breaches and immediately reporting actual or suspected data breaches in accordance with this DBP and all applicable obligations under the PPIP Act.

7 What is a data breach?

A data breach occurs when there is any unauthorised access, unauthorised disclosure or loss of personal information. A data breach may be deliberate or arise due to human error or accident.

Some examples of data breaches include:

- unauthorised access to Hunter Water's systems and associated data sets (for example, when a person's information is accessed by a hacker or other authorised party);
- sending an email or other communication to the wrong recipient;
- theft of personal information; or
- leaving a document or USB containing personal information in a public place.

However, a data breach can occur through various other channels.

8 What is an 'Eligible Data Breach?'

An 'eligible data breach' (known in this document as an EDB) is defined in section 59D of the PPIP Act as:

- Unauthorised access to, or unauthorised disclosure of, personal information held by Hunter Water and a reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to an individual to whom the information relates; or
- Personal Information held by Hunter Water is lost in circumstances where:
 - Unauthorised access to, or unauthorised disclosure of, the information is likely to occur; and
 - If the unauthorised access to, or unauthorised disclosure of, the information were to occur, a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to an individual to whom the information relates.

Whether there is a 'serious risk of harm' and whether an EDB has occurred must be assessed on a case-by-case basis. Harm to an individual may include (among other categories) financial loss, fraud, physical or emotional harm or reputational damage.

9 How Hunter Water Has Prepared for a Data Breach

Hunter Water has taken a privacy by design approach which embeds privacy management into all aspects of Hunter Water's operations through people, processes and systems.

Hunter Water has implemented controls, systems and processes to identify and prevent data breaches and to ensure that any data breach is effectively managed. These preventative measures include (among others), security and technical controls, bespoke plans, policies and procedures and contractual measures within its contracts with third parties. Hunter Water also provides ongoing staff training and awareness in relation to this DBP and the identification and response to data breaches.

The DBP forms part of Hunter Water's Privacy Framework and has been prepared in the context of Hunter Water's related plans and processes to ensure a comprehensive approach to preventing, mitigating and managing data breaches.

10 Reporting and Responding to a Data Breach

There are five key steps required in the response to a data breach or suspected data breach:

1. Report the breach internally;
2. Contain and mitigate the breach;
3. Assess the breach, including to determine if the breach is an EDB.
4. If the breach is found to be an EDB:
 - i. report the breach to the Privacy Commissioner; and
 - ii. notify affected persons, subject to exceptions under the PPIP Act
5. Post-breach review and evaluation.

In the unlikely event of multiple data breaches, Hunter Water will triage the breach based on the type and seriousness of the breach and the potential risk of harm. However, at all times, Hunter Water will ensure compliance with its legislative obligations, including under the PPIP Act.

10.1 Reporting the Breach

Hunter Water encourages the proactive and timely identification and reporting of privacy and data breaches. All data breaches involving data held by Hunter Water or affecting Hunter Water's data sets (including any customer or employee data) should be immediately reported to Hunter Water's Legal and Privacy Officer at hunterwaterprivacy@hunterwater.com.au].

Further, immediately upon becoming aware that there are reasonable grounds to suspect there may have been an EDB of Hunter Water, Hunter Water's people must report the matter to the Managing Director.

10.2 Assess the Breach

On receipt of the notification of a suspected or actual EDB, the Managing Director or the Managing Director's delegate must:

- immediately take all reasonable efforts to contain the data breach; and
- expeditiously and within 30 days (and whenever practicable, earlier):
 - carry out an assessment as to whether the breach is, or there are reasonable grounds to believe the breach is, an EDB; and
 - take all reasonable steps to mitigate the harm caused by the EDB or suspected EDB throughout the assessment.

To this end, the Managing Director may direct the DBRT to:

- carry out the assessment referenced above; and
- assist Hunter Water to contain and mitigate the breach (for example, to shut down any systems that have been breached, suspend the activity that led to the breach, revoke or change access codes or passwords).

Extension of the Assessment

If the Managing Director is satisfied that an assessment cannot reasonably be conducted within 30 days (Initial Period), the Managing Director may approve an extension for an amount of time reasonably required for the assessment to be conducted (Extension Period). If an Extension Period is approved, the Managing Director must, within the Initial Period:

- start the assessment; and
- give written notice to the Privacy Commissioner that the assessment has begun; that an extension has been approved by the Managing Director; and specify the new assessment period.

If the assessment is not conducted within the Extension Period, the Managing Director must, before the end of the extension period, give written notice to the Privacy Commissioner that the assessment is ongoing; a new extension has been approved; and specify the new extension period.

Note: Extensions of time should be a last resort. The timely assessment of suspected data breaches will assist Hunter Water to more quickly identify and assess the nature of the breach and to take the most appropriate steps to mitigate any potential harm caused by the breach.

Carrying Out the Assessment

The DBRT or relevant assessor is to consider the following factors in carrying out an assessment of a data breach:

- the types of personal information involved in the breach;
- the sensitivity of the personal information involved in the breach;
- whether the personal information is or was protected by security measures;
- the persons to whom the unauthorised access to, or unauthorised disclosure of, the personal information involved in the breach was, or could be, made or given;
- the likelihood the persons specified in the former bullet point:
 - have or had any intention of causing harm; or
 - could or did circumvent security measures protecting the information;
- the nature of the harm that has occurred or may occur; and
- any other matter set out in any Privacy Commissioner guidelines.

10.3 Report the breach to the Privacy Commissioner

If, following the assessment, the Managing Director believes there has been an EDB, the Managing Director must immediately notify the Privacy Commissioner of the EDB.

The notification to the Privacy Commissioner is to be made using the approved form published by the Information and Privacy Commission on its website.

The information requested by the approved form must be completed by Hunter Water unless it is not reasonably practicable for the information to be provided.

10.4 Notify affected persons

As soon as practicable after the Managing Director decides that an EDB has occurred, the Managing Director or delegate must, to the extent that it is reasonably practicable, take the steps that are reasonable in the circumstances to notify each individual to whom the personal information the subject of the breach relates or each affected individual.

That notification must include the following details to the extent it is reasonably practicable for the details to be provided:

- the date the breach occurred;
- a description of the breach;
- how the breach occurred;
- the type of breach that occurred (e.g. unauthorised disclosure, unauthorised access, or loss of information);
- the personal information that was the subject of the breach;
- the amount of time the personal information was disclosed for;
- actions that have been taken or are planned to ensure the personal information is secure, or to control or mitigate the harm done to the individual;
- recommendations about the steps the individual should take in response to the EDB;
- information about the making of privacy related complaints under Part 3, Division 3 of the PPIP Act and internal review processes under Part 5 of the PPIP Act;
- identifying Hunter Water as the entity the subject of the breach;
- if other public sector agencies are involved, the names of the other public sector agencies; and
- contact details for Hunter Water or a nominated contact person.

A template form of correspondence to affected individuals is provided at Appendix A to this DBP.

If the Managing Director is unable to provide a notification to an individual as required under section 59N of the PPIP Act, or if it is not reasonably practicable for the Managing Director to notify those individuals, the Managing Director must publish a notification on the public notification register to be kept by Hunter Water on its website . The notification must, if it is reasonably practicable for the information to be provided:

- be published on the public notification register for at least 12 months after the date the notification is published; and
- include the information specified in section 59O of the PPIP Act, except to the extent the information contains personal information or would prejudice Hunter Water's functions.

As soon as practicable after the notification is published, Hunter Water must notify the Privacy Commissioner about how to access the notification on the public notification register (eg by providing a link).

10.5 Ongoing review and reporting

Pursuant to section 59Q of the PPIP Act, the Managing Director must notify the Privacy Commissioner of any new information (that is, information that was not provided as part of the immediate notification under section 59M of the PPIP Act (as set out in section 10.3). The further information must be given following notification under sections 59N(1) or (2) of the PPIP Act, or, if applicable, once Hunter Water has determined that an exemption under Division 4 of the PPIP Act applies (outlined in section 11). This further information to the Privacy Commissioner must be provided in an approved form available on the Information and Privacy Commission's website.

11 Exemptions

11.1 Involvement of Multiple Agencies

If the EDB involves multiple public sector agencies, once each public sector agency has carried out an assessment and notified the Privacy Commissioner of an EDB, all heads or chief executive officers (as the case may be) need not provide notification to affected individuals or public notification, if the head of one public sector agency undertakes to do the notifications for all the affected public sector agencies.

11.2 Prejudice to Proceedings

The Managing Director does not have to carry out the notifications to individuals or public notifications to the extent that the Managing Director reasonably believes such notification would be likely to prejudice:

- an investigation that may lead to the prosecution of an offence;
- proceedings in a court or tribunal; or
- any matter prescribed in the *Privacy and Personal Information Protection Regulation 2019* (NSW).

11.3 Mitigation has been effective

If mitigating steps have been taken:

- in the case of unauthorised access to, or disclosure of, personal information:
 - if Hunter Water has taken action to mitigate the harm done by the breach;
 - if the mitigating action is taken before the unauthorised access or disclosure results in serious harm to an individual; and
 - because of the mitigation action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to an individual; or
- in the case of loss of personal information:
 - if Hunter Water take action to mitigate the loss;
 - if the mitigating action is taken before there is unauthorised access or disclosure of the information; and
 - there is in fact no unauthorised access to, or disclosure of, the information because of the mitigating action taken,

then the Managing Director does not have to provide notification to individuals or public notification.

11.4 Secrecy

If notification would be inconsistent with a secrecy provision of an Act or statutory rule, the Managing Director is exempt from the requirement to provide notification to individuals or public notification to the extent of the inconsistency.

11.5 Serious Risk of harm to health and safety

If the Managing Director reasonably believes that notification would create a serious risk of harm to an individual's health or safety, the Managing Director may exempt Hunter Water from the requirement to provide notification to individuals or public notification.

In making the decision, the Managing Director must:

- consider the extent to which the harm of notification is greater than the harm of not notifying;
- consider the currency of the information relied upon in assessing the serious risk of harm to an individual; and
- not search data held by Hunter Water, or permit such a search, that was not affected by the breach, to assess the impact of notification, unless the Managing Director knows or reasonably believes there is information in the data relevant to whether an exemption should apply.

The Managing Director must have regard to the guidelines prepared by the Privacy Commissioner in making a decision to exempt Hunter Water from notification under this section.

The exemption may be permanent, or for a specific period, or until the happening of a particular thing.

The Managing Director must, by written notice, notify the Privacy Commissioner that the exemption is relied on, provide details about whether the exemption is permanent or temporary, and if the exemption is temporary, provide details of the specified or expected time the exemption is to be relied upon.

11.6 Exemptions to prevent compromising cyber security

If the Managing Director reasonably believes that notification to an individual or public notification would worsen Hunter Water's cyber security or lead to further data breaches, then the Managing Director may decide to exempt Hunter Water from the requirement to provide notification to individuals or public notification, but only for as long as is necessary to prevent the situation worsening or leading to further data breaches.

In making the decision, the Managing Director must consider guidelines issued by the Privacy Commissioner. If the exemption is relied upon, the Managing Director must give written notice to the Privacy Commissioner, notifying:

- that an exemption under section 59X of the PPIP Act is relied on;
- when the exemption is expected to end; and
- the manner in which the exemption will be reviewed.

The Managing Director must review the exemption each month and provide an update to the Privacy Commissioner on the review of the exemption.

12 Post-breach review, evaluation and the Prevention of Future Repeat Data Breaches

If an EDB occurs, Hunter Water will conduct a post-breach review and evaluation to consider any learnings and potential areas for improvement. Hunter Water may also further investigate the circumstances of the breach to determine all causes and consider what short or long-term measures could be taken to prevent any reoccurrence.

Measures could include:

- more regular security audits of both physical and technical security controls;
- review of policies and procedures;
- review and revision of staff/contractor training practices; and/or
- review of contractual obligations with contracted third-party service providers.

13 External engagement

Where a data breach occurs, Hunter Water may need to engage with, or report the matter, to other external parties including law enforcement bodies and other regulators as required by law or as is necessary to best respond to, address and mitigate the breach.

In some instances, Hunter Water also needs to comply with the Commonwealth notifiable data breach scheme under the *Privacy Act 1988* (Cth), namely, in relation to data breaches involving tax file numbers.

Hunter Water may also have obligations under its contracts and arrangements with third parties which it will need to also consider.

14 Record keeping

Hunter Water will keep a record of data breaches and its response to data breaches as required by law and the MNDB Scheme. Hunter Water will also:

- maintain an internal register of EDBs; and
- where required, publish and maintain a 'public notification register' pursuant to section 59P of the PPIP Act.

15 Breaches of this DBP

Hunter Water takes privacy compliance seriously. A breach of this DBP or privacy by Hunter Water's employees may result in disciplinary action up to and including termination of employment (consistent with the Performance Management, Misconduct and Disciplinary Policy).

A breach of this DBP or contractual obligations of privacy by Hunter Water's contractors may result in Hunter Water taking various actions pursuant to the terms of the relevant contract and at law, which may result in (without limitation) termination of the contractor's engagement.

Any suspected breaches will be investigated in line with Hunter Water's Complaints and Allegations Policy.

16 Relevant Legislation, Policies and Guidance

Document ID	Document Title
Act	Privacy and Personal Information Protection Act 1998 (NSW)
Act	Government Information (Public Access) Act 2009 (NSW)
Act	Health Records and Information Privacy Act 2002 (NSW)
Policy	Privacy
Policy	Cybersecurity
Plan	Privacy Management Plan

Signed:

Jennifer Hayes
A/Chief Executive Officer

Approved By	A/Chief Executive Officer	Approved Date	12/Dec/2025
Maintained By	Privacy Officer & Legal Counsel	Next Scheduled Review Date	12/Dec/2029
TRIM File No.	HW2021-606/74.001	<i>(Note: Minimum review period 4 years)</i>	
Version	2		